Recorded Future Alerts - QRadar Installation Guide v1.0.1

- Application Description
- System Requirements
- Installation
- Configuration
 - · Creating an authorized service token
 - Importing Pulse dashboards
 - Custom Rules
 - Increase Max TCP Syslog Payload Length
 - Recorded Future Alerts configuration
- Application Functionality
 - Triage alerts
 - Triage using AQL
 - Fetch alerts
- Pulse dashboards
- Organisation Filter
 - Alert Rules List
 - Recorded Future Alerts Statistics
 - Recorded Future Alerts and Recorded Future Playbook Alerts
 - Recorded Future Domain Abuse
 - Recorded Future Domain Code Repository and Recorded Future Email Code Repository
 - Recorded Future Identify Similar Domains
 - Recorded Future Leaked Credential Monitoring and Recorded Future Leaked Email Monitoring
 - Recorded Future My domains on Dark Web and closed sources
 - Recorded Future Potential Logo Abuse Detection
 - Recorded Future Vulnerability Risk, New Critical or Pre NVD Watch List Vulnerabilities
- Supported Alerts
 - Mapping custom alerts using the DSM Editor
- Logging & Troubleshooting
 - Syslog connection issues
 - · Logs indicate alerts were sent to QRadar, but search returns no alerts
 - Truncation of events
 - Not fetching alerts
- Appendix
 - Supported Alert Rules
 - Out-of-the-box Custom Event Properties (CEP)

Application Description

Recorded Future is continuously harvesting data from Open, Deep, and Dark Web sources in real-time including Social media, Forums, Blogs, IRC channels, Paste sites, email groups, onion sites via TOR, and more through a range of collection mechanisms. Thousands of sources are added to our index for customers each week and are currently mining and cross-correlating data from over 750,000+ sources in seven languages with a patented Temporal Analytics[™] Engine.

The Recorded Future application for IBM QRadar enables:

- Delivery of Recorded Future Alert details consumed in IBM QRadar as events via custom Recorded Future log sources.
- Triaging Recorded Future Alerts and Playbook Alerts with the full alert details context directly in the IBM QRadar product.
- Review trending Inteligence Goals Library (IGL) data.

• Ability to document historial credential leaks.

The Recorded Future Alerts application for IBM QRadar enables better alerts triaging by adding relevant and comprehensive context.

System Requirements

- IBM QRadar version 7.4.1 Fix Pack 2 or higher
- IBM QRadar Authorized Services Token (Admin)
- Recorded Future Connect API Token
- TCP Port 514 open from QRadar server where the application is running to the syslog destination
- · Recorded Future account for accessing content when pivoting outside IBM QRadar to the Recorded Future platform

Installation

The preferred installation method for Recorded Future Alerts application is by uploading the application zip file via Extension Management.

Configuration

Once the Recorded Future Alerts application is installed, the "Settings" icon should be already visible under the "Admin" tab from IBM QRadar in the "Plug-ins" sections.

Before configuring the application itself, please complete these steps in the following order:

- 1. Creating an authorized service token
- 2. Importing Pulse dashboards
- 3. Custom Rules
- 4. Increase Max TCP Payload Length
- 5. Recorded Future Alerts configuration

≡	IBM QRadar						Ļ	<u> </u>
Dashboard	Offenses	Log A	ctivity	Admin	Pulse	Reference Data Management	System Time	: 17:24
Admin			🕙 Deploy (Changes	Advanced V			
System	m Configuration	<	1) There a	are no cł	nanges to depl	oy.		
► Data	Sources		Recorded	d Future	Alerts		 	
Remo Servio	te Networks and ces Configuration		• Se	ttings				
Try it	out			0				

Creating an authorized service token

The Recorded Future Alerts application requires an IBM QRadar Authorized Service Token (AST) to operate.

Note: QRoC customers get their AST from the "self Serve App" See: 📾 Authorized service tokens

Please use the following steps to create such a Token that you can later use in the application configuration window:

- 1. Click on the Admin tab
- 2. Click Authorized Services
- 3. Click +Add
- 4. In the Authorized Service Label, type a name for the authorized service
- 5. From the Security Profile list, select Admin
- 6. From the User Role list, select Admin
- 7. Set the desired token expiry period

Authorized Service	Mana	gement						?
Filter Search Results	5						New Authorized Servic	e X
User Role (1)		Search Authorized Service					Authorized Service Label recfut_alerts	
Admin	1	Authorized Service Label	User Role	Security Profile	Authorized By	Last Used	Permissions	
Admin	1	recfut_alerts	Admin	Admin	admin	Fri, 18/11/2022,	Security Profile Admin User Role Admin	Manage Security Profiles Manage User Roles
							Expiry Settings	
							Cancel	Save

8. Click Save

Once the service is created, the newly created **Authentication Token** is displayed and can be copied. Please note that, the authorized service token cannot be made visible after you close the **Authorized Service Created Successfully** dialog. Copy the token to a secure location before you close the dialog. Link for reference: Adding an authorized service

Importing Pulse dashboards

The application comes with a set of dashboards which allow to quickly visualise and effectively triage Recorded Future alerts & playbook alerts in the IBM QRadar Pulse application. To install the dashboards, please follow the steps detailed below:

- 1. Click on the Admin tab
- 2. Click Pulse Dashboard
- 3. Click Synchronize

Pulse Dashboard Templates

Name	Status
Recorded Future - Email Code Repository Alerts from Recorded Future. Email Code Repository alert rule.	New
Recorded Future - Identify Similar Domains	New
Recorded Future - Potential Logo Abuse Detection	New

- 4. Click on the Pulse tab
- 5. Click on the **Dashboard** dropdown
- 6. Click Create Dashboard

Dashb	ooard	Offenses	Log Activity	Admin	Pulse	Reference Data Management	
¢٩	Dashbo Recor	oard ded Future	- Alert Details	^			
Para ★ Ti	Q	Search fo	r dashboards				\ ছি ~
1	Event Use th	and flow m	n etrics lashboards as a	starting po	int to crea	te your own customized dashboards.	ľ
Aler -≎	Misce Use th	e llaneous m ese default c	etrics lashboards as a	starting po	int to crea	te your own customized dashboards.	
	Offen Use th	se overview ese default c	/ lashboards as a	starting po	int to crea	te your own customized dashboards.	
	Recor	ded Future	- Admin Dashl	board A			
	Recor	ded Future	- Alert Details	ዖ			~
	Recor	ded Future	- Domain Cod	e Reposit	ory A		
	Creat	e dashboar	d				

7. Click Manage templates

8. Click Install for each Recorded Future named dashboard

Custom Rules

The application comes with a set IBM QRadar Offense Rules to enable offense generation. These rules can be found in the **Recorded Future Alerts** group.

By default these rules are enabled and will generate an offense per Recorded Future alert.

Non parsing alerts will not generate offenses.

Increase Max TCP Syslog Payload Length

Because alerts and playbook alerts are sent via syslog and some of the alert payloads can be rather large, this can easily top the QRadar default settings for the Max TCP Syslog Payload Length. This will result in some Recorded Future alert payloads being truncated and not parsing correctly. To avoid this issue from happening, follow the steps outlined below:

- 1. Click on the Admin tab
- 2. Click System Settings
- 3. Click Advanced
- 4. In the Max TCP Syslog Payload Length field, type 12288

System Settings

oystem oettings				
Sustem Settings	Global Iptables Access (comma separated)			
System Settings	Syslog Event Timeout (minutes)	720	*	
Database Settings	Partition Testers Timeout (seconds)	30	-	
Ariel Database Settings	Max UDP Syslog Payload Length	2,048	-	
Custom Bula Sattinga	Max TCP Syslog Payload Length	12,288	-	
Custom Aule Settings	Max Number of TCP Syslog Connections	2,500	÷	
Transaction Sentry Settings	Max TCP Syslog Connections Per Host	10	\$	
SNMP Settings	Timeout for Idle TCP Syslog Connections (seconds)	900	-	
Embedded SNMP Daemon Settings	Log and Network Activity Data Export Temporary Directory	/store/exports		

- 5. Click Save
- 6. The changes made will require a Full Deploy, click on the Admin tab
- 7. From the Advanced list, click Deploy Full Configuration

8. After services restart, the QRadar deployment is updated to allow TCP packets that are up to 12288 bytes without truncation

🚯 More information about the topic QRadar: TCP and UDP Syslog Maximum Payload Message Length for QRadar Appliances

Recorded Future Alerts configuration

The configuration page for the Recorded Future Alerts application can be found in the **Admin** tab within the **Plug-ins** section. Once opened the configuration page will enable configuration of the following parameters:



· Logs - links to application logs

Recorded Future API

- API Key Recorded Future API Token
- SSL verification switch Allows to disable SSL certificates verification when reaching out to the Recorded Future API

IBM QRadar

- Syslog Destination IP/Hostname of a QRadar syslog destination which the Recorded Future Alerts application uses to send alerts as events via syslog on port 514.
- Authorization Token IBM QRadar Authorized Service Security Token created in the previous steps

Recorded Future Alerts

- Fetch Alerts switch when disabled Recorded Future Alerts will not be downloaded
- Fetch Playbook Alerts switch when disabled Recorded Future Playbook Alerts will not be downloaded
- Alert Poll Frequency controls how often the alerts & alert updates (applicable to Playbook Alerts) be ingested. Defaults to 60 minutes, lowest supported interval is 15 minutes.
- · Alerting Rules list selected alerting rules will be ingested
- · Playbook Alerts list selected playbook alerts will be ingested

(i) List of alert rules to select will only be available once the configuration has a valid Recorded Future API Key saved.

Application Functionality

Recorded Future Alerts application's functionality is underpinned by the Recorded Future API, which is the repository from which QRadar retrieves the Recorded Future Alerts and Playbook Alerts. The app fetches alert details and provides them to QRadar via two log sources **Recorded Future Alerts** and **Recorded Future Playbook Alerts**. This makes the alerts context ready for triaging and advanced correlation in IBM QRadar.

Triage alerts

Ingested alerts become searchable with the help of AQL queries and a set of Pulse dashboards detailed later in this document.

Triage using AQL

The query below returns all ingested Recorded Future Alerts from the past 3 days.

```
1 SELECT
     "Alert ID",
2
     "Alert Title" AS "Alert Title",
3
4
     DATEFORMAT("Alert Triggered Time", 'yyyy-MM-dd hh:mm:ss') AS 'Triggered Time',
5
      "Alert URL" AS 'Alert URL',
     logsourcename(logsourceid) AS log_source_name
6
7 FROM events
8 WHERE (
9
       log_source_name = 'Recorded Future Alerts'
10 )
11 GROUP BY "Alert ID"
12 ORDER BY "Triggered Time" DESC last 3 Days
```

The query below returns all ingested Recorded Future Playbook Alerts from the past 3 days.

```
1 SELECT
2
    "Entity Name" AS "Entity Name",
     "Alert ID",
3
     DATEFORMAT("Alert Triggered Time", 'yyyy-MM-dd hh:mm:ss') AS 'Triggered Time',
4
       "Alert URL" AS 'Alert URL',
5
     logsourcename(logsourceid) AS log_source_name
6
7 FROM events
8 WHERE (
9
     log_source_name = 'Recorded Future Playbook Alerts'
10 )
```

11 GROUP BY "Alert ID"
12 ORDER BY "Triggered Time" DESC last 3 Days

The query below returns all email addresses and passwords that have been leaked with the market name where they are sold.

```
1 SELECT
2 "Email Leaked" AS "Leaked Email",
3
     "Leaked Password",
     "Alert Source Name" AS "Source Name",
4
5
     DATEFORMAT("Alert Triggered Time", 'yyyy-MM-dd hh:mm:ss') AS 'Triggered Time',
6
     logsourcename(logsourceid) AS log_source_name
7 FROM events
8 WHERE (
9
      "Alert Rule Name"='Leaked Credential Monitoring' AND
     log_source_name = 'Recorded Future Alerts'
10
11 )
12 ORDER BY "Triggered Time" DESC last 3 DAYS
```

The query below returns all the similar domains (example typosquats) that have been seen in the last 3 days.

```
1 SELECT
2 "Alert Source Name" AS "Repo Name",
     "Similar Domain" AS "Domain",
3
4
     DATEFORMAT("Alert Triggered Time", 'yyyy-MM-dd hh:mm:ss') AS "Triggered Time",
     logsourcename(logsourceid) AS log_source_name
5
6 FROM events
7 WHERE (
8
      "Alert Rule Name"='Identify Similar Domains' AND
     log_source_name = 'Recorded Future Alerts'
9
10 )
11 ORDER BY "Triggered Time" DESC last 3 DAYS
```

The query below returns a list of target domains that have been triggered by the domain abuse playbook alert in the last 3 days.

```
1 SELECT
2 "Entity Name" AS "Domain",
     "Targets List" AS "Target",
3
4
      DATEFORMAT("Alert Triggered Time", 'yyyy-MM-dd hh:mm:ss') AS 'Triggered Time',
     logsourcename(logsourceid) AS log_source_name
5
6 FROM events
7 WHERE (
8
     "Alert Rule Name" = 'Domain Abuse' AND
     log_source_name = 'Recorded Future Playbook Alerts'
9
10 )
11 ORDER BY "Triggered Time" DESC last 3 DAYS
```

Fetch alerts

The users can trigger an alert poll ahead of schedule from the Offenses tab.

	/I QRadar						
Dashboard	Offenses	Log Activity	Network Activity	Admin	Pulse	Reference Data Management	QDI
Offenses		Search	 Save Criteria 	Actions V	🗁 Print 📲	Refresh Recorded Future Alerts	
My Offens	ses						

Please note in may take some time before new alerts become searchable in QRadar as the system can take time to process the events. The exact amount of time depends on the size and load of the QRadar deployment.

Pulse dashboards

Some tables in the dashboards will not present data straight away. It is require that you select the row (alert) that you are interested into to get the details in the subsequent tables.

Also note that for more details all the dashboards link back to the Recorded Future App. A valid Recorded Future account is needed to see those details.

Below are reported all the actions that you can perform without having access to the Recorded Future App.

Organisation Filter

Every user will have a filter called "Organisation" in each dashboard. This is used to filter for specific Recorded Future Alerts based on the Organisation in which the alert triggered. To select an organisation, just enter a part of the organisation name and click Update

Organisation	Time Value	★ Time Period	
Org1	10	Days	Update

If you want to see all the alerts from all the organisations, enter a dot (.)



If you do not have Multi-Org enabled in the Recorded Future Portal, just configure the Organisation filter, with the dot (.) character:

- In the top right side click on the three dots
- Click on Manage Parameters



- Search for "Organisation"
- Set "Default value" as .
- Click Save

Alert Rules List

Below is the list of Alert Rules, both legacy and playbook alerts, that you will find out of the box.

- Domain Abuse
- Domain Code Repository
- Email on Code Repository
- Identify Similar Domains
- Leaked Credential Monitoring
- Leaked Email Monitoring
- My domains on Dark Web and closed Sources
- New Critical or Pre NVD Watch List Vulnerabilities (Global)
- New Critical or Pre NVD Watch List Vulnerabilities (Tech Stack)
- Potential Logo Abuse Detection

Recorded Future Alerts Statistics

This dashboard shows the number of alerts that failed to be ingested in the Alerts - Unknown Events and Playbook Alerts - Unknown Events , the number of total alert ingested for both Legacy and Playbook and the Timeline of the ingested alerts.



Recorded Future Alerts Statistics

Recorded Future Alerts and Recorded Future Playbook Alerts

These two dashboards show an overview of the alerts that have been parsed.

Recorded Future Alert	s ~					_	8 ₈
			Days	qR7hRb			
Alert Details - Latest Alerts T A few seconds ago Triggered Time	friggered Alert ID	Alert Title			Organisation - Owner		Alert Details - Latest Alerts Triggered - Count :
Mar 07, 2023, 10:11 AM	qR7hRc	Banking and Paym	ents, Trending Targets in Banking & F	ayments - Spike	Professional Services Developm	ent - Professional Services Development	
Mar 07, 2023, 10:10 AM	qR7hRZ	Cyber Espionage, R	elated Targets - Rise: Pok\u00e9mo	n, Redis, Indone	Professional Services Developm	ent - Professional Services Development	
Mar 07, 2023, 10:10 AM	qR7hRb	Cyber Events affect	ing my Brands - 2 new references in	2 documents	Professional Services Developm	ent - Professional Services Development	
Mar 07, 2023, 10:10 AM	qR7hRT	Brand on Cyber-Fo	cused Messaging Channels - 64 new	references in 6	Professional Services Developm	ent - Professional Services Development	
Mar 07, 2023, 10:10 AM	qR7hRW	ICS/SCADA, ICS M	alware, RATs - Rise: SysUpdate and E	IARAT	Professional Services Developm	ent - Professional Services Development	
Mar 07, 2023, 10:10 AM	qR7hRU	Banking and Paym	ents, Malware Used in Banking & Pay	ments Cyber Att	Professional Services Developm	ent - Professional Services Development	
Mar 07, 2023, 10:10 AM	qR7hRK	Brand name in sus	picious websites content (OCR) - 100	0+ new referen	Professional Services Developm	ent - Professional Services Development	
Displaying 250 of 1000 rows							
Alert Details - Latest Alerts 1 A few seconds ago	friggered - Detail	5					
Triggered Time	Alert Rule Name		Fragment				
Mar 07, 2023, 10:10 AM	Cyber Events at	fecting my Brands	Mir\u00e1 que hay cosas para haci	iear, y me hackean la	cuenta de Netflix.		
Mar 07, 2023, 10:10 AM	Cyber Events al	fecting my Brands	Insikt Group Analysis Report - Targ	ets: Coinbase Global,	, Inc., Twilio, CloudFlare; Methods	s: T1078, T1566.002, T1566.003, T1589; (Operation: Oktapus
Mar 07, 2023, 10:10 AM	Cyber Events at	flecting my Brands	Insikt Group Analysis Report - Targ	ets: Coinbase Global,	Inc., Twilio, CloudFlare; Methods	s: T1078, T1566.002, T1566.003, T1589; (Operation: Oktapus
Mar 07, 2023, 10:10 AM	Cyber Events at	ffecting my Brands	Mir\u00e1 que hay cosas para haci	ear, y me hackean la	cuenta de Netflix.		

In the dashboard above, clicking on any of the alerts in the Alert Details - Latest Alerts Triggered will populate the widget below it (Alert Details - Latest Alerts Triggered - Details) with details on the specific alert.

Recorded Future Playbook	Alerts ~								۲	R.R. 2	t C	1
Parameters												о ×
Organisation												
14 C			Days									
Playbook Alert Details - Latest Al	erts Trigge	red						Playbook Alert Details - Late	est Aler	ts Trigg	ered - C	o
A rew seconds ago	Entity							A few seconds ago				
Entity	Risk Score	Targets List			Triggered Time	Updated Time	Organisation Name					
dier.me	26	"ideodlor.me", "ideodl	er.com*		Mar 07, 2023, 04:41 AM	Mar 07. 2023. 04:58 AM	Professional Services Development				N	
email com socoanel com		*ide:email.com*			Mar 07 2023 04:32 AM	Mar 07 2023 04-32 AM	Professional Services Development					
www.dmail.com.comanel.com		*ideutmail.com*			Mar 07, 2022, 04:32 AM	Mar 07, 2023, 04:32 AM	Professional Services Development					
www.gnail.com.socpanet.com		Education and Educ			Mai 07, 2023, 04.32 AM	Har 07, 2023, 04.32 MH	Professional Genvices Development					
soty.com		"idn:doty.com", "idn:	sotby.com, ion:saoty.com, ion:sony.com	, 10	Mar 07, 2023, 03:15 AM	Mar 07, 2023, 03:15 AM	Professional Services Development					
www.gmail.ngrok.app		"idn:www.gmail.cl", "	idn:www.gmail.at", "idn:www.gmail.ca", "idi	n:ww	Mar 06, 2023, 10:51 PM	Mar 06, 2023, 10:51 PM	Professional Services Development		67			
www.gmail.ngrok-free.dev		"idn:www.gmail.cl", "	idn:www.gmail.at", "idn:www.gmail.ca", "idr		Mar 06, 2023, 10:51 PM	Mar 06, 2023, 10:51 PM	Professional Services Development					
www.gmail.ngrok.dev		"idn:www.gmail.cl", "	idn:www.gmail.at", "idn:www.gmail.ca", "idi		Mar 06, 2023, 10:42 PM	Mar 06, 2023, 10:42 PM	Professional Services Development	Domain Abuse				
email.lvchadizhi.at.gmail.com.		"idn:gmail.com"			Mar 06, 2023, 06:57 PM	Mar 06, 2023, 06:58 PM	Professional Services Development					
recordedfuture.sk		"idn:recordedfuture.c	n", "idn:recordedfuture.co.kr", "idn:recorde	dfut	Mar 06, 2023, 05:30 PM	Mar 06, 2023, 06:06 PM	Professional Services Development					
recordedfuture.uk		*idn:recordedfuture.c	n", "idn:recordedfuture.co.kr", "idn:recorde	dfut	Mar 06, 2023, 05:30 PM	Mar 06, 2023, 06:15 PM	Professional Services Development					
anpplus.com		"idn:andplus.com", "i	dn:fnpplus.com", "idn:applus.com", "idn:ant	tplus	Mar 02, 2023, 04:52 AM	Mar 06, 2023, 12:24 AM	Professional Services Development					
api.gmall.com		"idn:api.vmall.com", '	'idn:api.gmail.com"		Feb 11, 2023, 03:55 PM	Mar 06, 2023, 04:05 AM	Professional Services Development					
fbwins.s3.amazonaws.com		"idn:fbwins.info"			Oct 12, 2022, 09:32 PM	Mar 07, 2023, 10:33 AM	Professional Services Development					
mypatpal.com		"idn:mypaypal.com"			Jul 29, 2022, 08:26 AM	Mar 05, 2023, 09:59 PM	Professional Services Development					
kelecloud.com		"idn:helecloud.com",	"idn:relectoud.com"		Jul 17, 2022, 11:57 AM	Mar 06, 2023, 10:50 AM	Professional Services Development					
xamobile.com		"idn:xnamobile.com"	, "idn:tamobile.com", "idn:camobile.com", "i	idn:e	Jul 15, 2022, 05:35 PM	Mar 06, 2023, 04:21 AM	Professional Services Development					
fast.tm		"idn:fast.co", "idn:fas	Lcom.tw", "idn:fast.no", "idn:fast.org", "idn:	fast	Jul 13, 2022, 12:47 AM	Mar 06, 2023, 04:07 PM	Professional Services Development					

Recorded Future - Domain Abuse

This dashboard shows the details of each domain abuse alert that has been received. Clicking on an alert in the Domain Abuse - Summary will populate the underlying tables with the details of the Whois data, DSN, MX and NS records.

- Domain Abuse Domain Whois will redirect you to the the Recorded Future portal a valid account is required to view the full alert and the screenshot. The column screenshot will give you an idea if there is a screenshot or not with the values Retrieved / Not Found
- Domain Abuse Domain DNS Records will redirect you to the enrichment of the A Record IP. The geolocation on the right side is provided by QRadar GEO::LOOKUP and it is related to the location of the IP.
- Domain Abuse Domain MX and NS Records shows the details of the MX Domain and IP, along with a list of NS Names.

≡ IBM QRadar								(III)	Ļ	<u>0</u>
Dashboard Offenses Log A	ctivity Admin Pulse Ref	erence Data Management						s	ystem Time: (09:26
Recorded Future - Dom	nain Abuse 💙							۶ _R	£ Ľ	
Parameters									ຄ	
+ Organisation	Time Value	🛨 Time Period	Domain Filter							
	10	Days	zyvc.com							
Domain Abuse - Count : A few seconds ago	Domain Abuse - Summary A few seconds ago									
	Triggered Time	Updated Time	Domain		Context	Risk Score	Target			
	Jul 06, 2022, 07:43 PM	Feb 25, 2023, 02:45 PM	fast.cyou		"Phishing Host"		"idn:fast.co", "idn:fast.co	n.tw", "	idn:fast.no	o", "id
560	Aug 03, 2022, 12:58 AM	Feb 25, 2023, 03:05 PM	venmopay.mobi		N/A		"idn:venmopay.org", "idn:	venmop	ay.net"	
509-	Oct 14, 2022, 05:48 AM	Feb 25, 2023, 03:22 PM	linaray.com		"Phishing Host"		"idn:linapay.com"			
	Jul 29, 2022, 08:26 AM	Feb 25, 2023, 05:31 PM	mypatpal.com		"Phishing Host"		"idn:mypaypal.com"			
	() Displaying 250 of 1000 rows									
Domain Abuse - Domain Who	is Link to Alart in Portal									
A few seconds ago	Context		Country	State	City	Name	Screenshot			
zvvc.com	"Phishing Host"		China	othic	sity.		Retrieved			
2)10:00	"Phishing Host"		China				Retrieved			
zyve.com	"Phiching Host"		China				Potriound			
zyvc.com	"Dhishing Host"		China				Retrieved			
zyvc.com	Phisning Host		China				Retrieved			
zyvc.com	"Phishing Host"		China				Retrieved			
Domain Abuse - Domain DNS A few seconds ago	Records Link to IP Enrichme	nt			Domain Abuse - Domain D A few seconds ago	ONS Records on Ma	p			
Domain A Re	ecord IP	IP Risk Score	IP Info							
zyvc.com 199	.59.243.222	50	"C&C Server"				10 minor	22	~~~~~	
zyvc.com 199	.59.243.222	46	"C&C Server"		- Say	1 and 1	2 A Francis		S.	3
zyvc.com 162	.55.217.94		"Phishing Host"		A.	2	KERDA	n.	28 al	
zyvc.com 162	.55.217.94		"Phishing Host"		· 3	for the second s	SELEC V	Ę,	R	
zyvc.com						337	E.S.	10		
						- PY	AND O			
						¥-				
						~e				2
Domain Abuse - Domain MX a	nd NS Records									
A few seconds ago										
Domain MX R	Record MX Risk Sc	ore MX Info	NS Names							
zyvc.com			["idn:contact.sk	ype.id.18606	5008806.myym.com", "idr	n:contact.wechat.or	r.qq.id.5300066.myym.coi	n", "idn	contact.w	/h
zyvc.com			["idn:contact.sk	ype.id.18606	5008806.myym.com", "idr	1:contact.wechat.or	r.qq.id.5300066.myym.coi	n", "idn	contact.w	
zyvc.com			["idn:contact.sk	ype.id.18606	5008806.myym.com", "idr	n:contact.wechat.or	r.qq.id.5300066.myym.co	n", "idn	contact.w	
zyvc.com			["idn:contact.sk	ype.id.18606	5008806.myym.com", "idr	n:contact.wechat.or	r.qq.id.5300066.myym.co	n", "idn	contact.w	
zyvc.com			["idn:contact.sk	ype.id.18606	6008806.myym.com", "idr	n:contact.wechat.or	r.qq.id.5300066.myym.co	n", "idn	contact.w	



Recorded Future - Domain Code Repository and Recorded Future - Email Code Repository

These two dashboards have the same layout and represent the domains and email seen in code repositories. The search filter applies for both full URLs, domains or part of the domains. In the example in the Domain Code Repository we have used instagram as a filter search. We could have used something more specific like instagram.com or https://www.instagram.com/shannon.art_/. The same applies for the Email Code Repository which takes part of the email, the full address or the domain.

The Domain Filtered and Email Filtered tables have been created with the idea of showing all the alerts involving a specific domain or email. Clicking on any entry in that table will redirect you to the alert in the Recorded Future Portal.

Example of Recorded Future - Domain Code Repository below:

Dashboard Recorded Future - Domain	n Code Repository							\$ 14	1 C
ameters									Ð
rganisation									
		Days	splunk						
nains on Code Repo - Details v seconds ago									
iggered Time	Domain	Repo Name F	ragment			Author	Organisation - Owner		
ar 07, 2023, 10:05 AM	2023-02-14.json	GitHub 2	023-02-14.json say:	s it stopped largest I	DDoS attack on record\": \"http	Lilenglun	Professional Services Developmen	- Professional Servic	es Developmer
ar 07, 2023, 10:05 AM	2023-02-23.json	GitHub 2	023-02-23.json \": \	"https://therecord.n	nedia/russia-radio-hackers-fa.	Lilenglun	Professional Services Developmen	- Professional Servic	es Developmer
ar 07, 2023, 10:05 AM	2022-10-25.md	GitHub 2	022-10-25.md claim	ns attack on Wiscon	sin school district](https://ther.	Lilenglun	Professional Services Developmen	- Professional Servic	es Developmer
ar 07, 2023, 10:05 AM	settings.py	GitHub s	ettings.py ')) SOCIAL	_AUTH_GOOGLE_O	AUTH2_SECRET = str(os.geten	Annymars23	Professional Services Developmen	t - Professional Servic	es Developmer
ar 07, 2023, 10:05 AM	bookshop-site-data.json	GitHub b	ookshop-site-data.js	son ://akash-writes.r	medium.com/\",\"works_butto.	akashTheCommunityGuy	Professional Services Developmen	- Professional Servic	es Developmer
ar 07, 2023, 10:05 AM	Virtual_keyboard.md	GitHub V	irtual_keyboard.md	: Tutorial Part 1: http	ps://medium.com/@wang33he	yushan1089	Professional Services Developmen	- Professional Servic	es Developmer
ar 07, 2023, 10:05 AM	CyberSecurityRSS-tiny.opml	GitHub C	yberSecurityRSS-tin	y.opml =\"rss\" htm	lUrl=\"http://regilero.github.io\	Lilenglun	Professional Services Developmen	- Professional Servic	es Developmer
ar 07, 2023, 10:05 AM	S-bash-approvalgates-5691-0014	i.yml GitHub S	-bash-approvalgates	s-5691-0014.yml @	gmail.com - email@example.c.	jfbetapipeorg	Professional Services Developmen	- Professional Servic	es Developmer
ar 07, 2023, 10:05 AM	u6c42.txt	GitHub P	HP\u6784\u9020htt	tp\u5934\u53d1\u9	001\u8bf7\u6c42.txt (\$_REQ.	tophub100	Professional Services Developmen	- Professional Servic	es Developmer
Displaying 250 of 1000 rows									
nains on Code Repo - Repo	. ; Domains on Code Repo - D	omain Filtered							۷
	Triggered Time	Domain	Repo Name	Author	Fragment		Repo URL		
	Mar 05, 2023, 10:03 AM	splunk-enterprise-panel.y	aml GitHub	ictmuzi	splunk-enterprise-panel.ya	ml id: splunk-enterprise-panel info: I	na https://github.com/ictmuzi/l	luscan/blob/master/t	tools/nuclei-te.
	Mar 05, 2023, 10:03 AM	splunk-enterprise-panel.y	aml GitHub		splunk-enterprise-panel.ya	ml id: splunk-enterprise-panel info: i	na		
	Feb 24, 2023, 10:04 AM	splunk.go	GitHub	steevex35	splunk.go /open-telemetry/	opentelemetry-collector-contrib/tes	st https://github.com/steevex3	5/opensearchexporte	r/blob/main/te
	Feb 16, 2023, 10:04 AM	webpack.splunkapp	GitHub		webpack.splunkapp.config.	js = require('@splunk/webpack-conf	fig		
	Feb 16, 2023, 10:04 AM	splunk_create.conf	GitHub	marcusschiesser	splunk_create.conf # this fi	le is generated by @splunk/create as	ut https://github.com/marcuss	hiesser/kveditor/blob	b/master/splun
	Feb 16, 2023, 10:04 AM	splunk.env	GitHub	marcusschiesser	splunk.env SPLUNK_PASSW	/ORD=splunkdev SPLUNK_START_AF	R https://github.com/marcuss	hiesser/kveditor/blob	b/master/splun

Recorded Future - Domain Code Repository

Recorded Future - Identify Similar Domains

Similar to the above dashboards, the Identify Similar Domains shows alerts triggering from the homonym alert. The Domain Filter works the same as the "Recorded Future - Domain Code Repository" dashboard.

Recorded Future - Ider	ntify Similar Domains 💙					\$^^ @	C 12 I
Parameters							ο×
+ Organisation							
		Days	splunk				
Identify Similar Domains - De	tails						:
Triggered Time	Domain		Fragment		Source Name	Organisation - Owner	
Mar 07, 2023, 10:08 AM	testing.splunkable.com		A certificate for the domain testing.splunka	able.com has been regist	New Certificate Registration	ns Professional Services Development - Professional Servic	es Develo
Mar 07, 2023, 10:08 AM	splunkhf01.samaritan.org		A certificate for the domain splunkhf01.sar	maritan.org has been reg	New Certificate Registration	ns Professional Services Development - Professional Service	es Develo
Mar 07, 2023, 10:08 AM	splunk.dev-fy37.staging.anywhere.	roche-digital.cn	A certificate for the domain splunk.dev-fy3	7.staging.anywhere.roc	New Certificate Registration	ns Professional Services Development - Professional Service	es Develo
Mar 07, 2023, 10:08 AM	splunk.tara-analytics.de		A certificate for the domain splunk.tara-an	alytics.de has been regis	New Certificate Registration	ns Professional Services Development - Professional Servic	es Develo
Mar 07, 2023, 10:08 AM	scde-wl3k3yebiwglwe6xp.splunkcl	oud.com	A certificate for the domain scde-wl3k3yet	biwglwe6xp.splunkcloud	New Certificate Registration	ns Professional Services Development - Professional Servic	es Develo
Displaying 250 of 492 rows							
Identify Similar Domains - So	ur Identify Similar Domains	- Domain Filtered					1
	A few seconds ago	Demois .					
	Inggered time	Uumain		Source Name	Fragme	n.	
400	Mar 07, 2023, 10:08 AM	testing.splunkable.com		New Certificate Re	gistrations A certif	licate for the domain testing.splunkable.com has been registere	đ
100	Mar 07, 2023, 10:08 AM	splunkhf01.samaritan.o	rg	New Certificate Re	gistrations A certif	licate for the domain splunkhf01.samaritan.org has been registe	red
	Mar 07, 2023, 10:08 AM	l splunk.dev-fy37.staging	, anywhere.roche-digital.cn	New Certificate Re	gistrations A certif	icate for the domain splunk.dev-fy37.staging.anywhere.roche-	figital.cn h
200	Mar 07, 2023, 10:08 AM	splunk.tara-analytics.de		New Certificate Re	gistrations A certif	icate for the domain splunk.tara-analytics.de has been register	ed
100	Mar 07, 2023, 10:08 AM	scde-wl3k3yebiwglwe6	xp.splunkcloud.com	New Certificate Re	gistrations A certif	icate for the domain scde-wl3k3yebiwglwe6xp.splunkcloud.cor	n has bee
	Mar 07, 2023, 10:08 AM	netsplunkui-02.rb2g.ru		New Certificate Re	gistrations A certif	icate for the domain netsplunkui-02.rb2g.ru has been registere	d
New Domain Registratio	Mar 07, 2023, 10:08 AM	30.stage-splunk.messa	gegearslabs.com	New Certificate Re	gistrations A certif	icate for the domain 30.stage-splunk.messagegearslabs.com h	as been re
New Certificate Registra	ions () Displaying 250 of 486 row						

Recorded Future - Identify Similar Domains

Recorded Future - Leaked Credential Monitoring and Recorded Future - Leaked Email Monitoring

These two dashboards work in the same way as well. Both the dashboards allow to filter for Email which will populate the Filter by Email table (bottom) or the Filter by Market table on the right. Both filters allow free-text of the whole Email/Market name or part of it. In the example we have used tesla as a search filter. The idea is to enable you to search for all the activities in a specific Market or for a specific email address or mail domain.

Leaked password in Leaked Email Monitoring might not be present due to the nature of the alert. There is a chance that an API Key will be captured by the alert rule. If that is the case it will be displayed with the text POSSIBLE API KEY LEAKED and it is required for you to log into the Recorded Future app to see the details.

	Leaked Emails - Overview A few seconds ago		Ø	:
	Nov 21, 2022			
	Nov 21, 2022			
	Nov 21, 2022			
	Nov 20, 2022	POSSIBLE API KEY LEAKED		
	Nov 20, 2022	And and a second se		
100	Nov 20, 2022			
9	Nov 20, 2022	- Manager and American Street St		
94 34	Nov 20, 2022			I
ю 6	① Displaying 250 of 276 row	\$		

Recorded Future - Leaked								© *x	
Parameters									
		Days	Cracked Forum		gmail				
Leaked Credentials - Counts 🧷	E Leaked Crede	ntials - Overview							
	Triggered Tir	ne Leaked Email		Leai	ied Password	Organisation - Owner			
		13 Il.com							
2072		13 gmail.com							
275		gmail.com		Pigg					
274 Cracked Forum	Mar 07, 202	13 il.com							
Nulled Forum	Mar 07, 202	13 mail.com							
Pastebin Poland	Mar 07, 202	13 L.com							
GitHub		13 gmail.com							
PasteBin January 2023 Combo Lists									
Leaked Credentials - Filter By Em	wil				Leaked Credentials	- Filter By Market			
Triggered Time	Source Name	Leaked Email	Leaked Password	Alert ID	Triggered Time	Leaked Email	Leaked Password	Source Name	Alert ID
		nail.fr				@gmail.com			
		5@gmail.co				and a lil.com			
		100 C				gmail.com			
		il.fr				gmail.com			
		Sgmail.co				gmail.com			
		@gmail.co				@gmail.com			
		and the second sec				gmail.com			

Recorded Future - My domains on Dark Web and closed sources

With this dashboard you will see a list of all the sources that triggers the alert with a counter of the number of alert that triggered. Clicking on each column will show the Fragment of the alert to give you a brief idea of what the alert is about. Clicking on the alert row itself will redirect you to the portal.



Recorded Future - My domains on Dark Web and closed sources

Recorded Future - Potential Logo Abuse Detection

This dashboard will provide value if you have access to the Recorded Future App since clicking on any row will link you directly to the screenshot taken from page that has your company logo on it.

Dashboard Recorded Future - Potentia	al Logo Abuse Detection 💙				Ę	≥ ^x	£	ß
ameters								Ð
rganisation								
		Days						
ential Logo Abuse Detection -	Details							
v seconds ago								
iggered Time	Malicious URL		~	ert URL	Organisation - Owner			
ar 07, 2023, 10:08 AM	http://hardrockhotel.fr/		ht	tps://app.recordedfuture.com/live/sc/notification/?id=qR7g8n	Professional Services Development - Professional Serv	ices Dev	elopme	nt
ar 07, 2023, 10:08 AM	http://2020tokyoolympic.com/		ht	tps://app.recordedfuture.com/live/sc/notification/?id=qR7g8n	Professional Services Development - Professional Services	ices Dev	elopme	nt
ar 07, 2023, 10:08 AM	http://shoping.center/		ht	tps://app.recordedfuture.com/live/sc/notification/?id=qR7g8n	Professional Services Development - Professional Services	ices Dev	elopme	nt
ar 07, 2023, 10:08 AM	http://ns12.mgtwzp.site/		ht	tps://app.recordedfuture.com/live/sc/notification/?id=qR7g8n	Professional Services Development - Professional Services	ices Dev	elopme	nt
ar 07, 2023, 10:08 AM	https://redirectings.info/Allgiftca	ardgiveaways?s1=PIR\$ING	ht	tps://app.recordedfuture.com/live/sc/notification/?id=qR7g8n	Professional Services Development - Professional Services	ices Dev	elopme	nt
ar 07, 2023, 10:08 AM	http://www.bankwezen.xyz/		ht	tps://app.recordedfuture.com/live/sc/notification/?id=qR7g8n	Professional Services Development - Professional Services	ices Dev	elopme	nt
ar 07, 2023, 10:08 AM	https://facebook.oia.bio/yb5hz		ht	tps://app.recordedfuture.com/live/sc/notification/?id=qR7g8n	Professional Services Development - Professional Services	ices Dev	elopme	nt
ar 07, 2023, 10:08 AM	http://pma.dorue.site/		ht	tps://app.recordedfuture.com/live/sc/notification/?id=qR7g8n	Professional Services Development - Professional Services	ices Dev	elopme	nt
ar 07, 2023, 10:08 AM	http://nycconfidential.com/		ht	tps://app.recordedfuture.com/live/sc/notification/?id=qR7g8n	Professional Services Development - Professional Services	ices Dev	elopme	nt
ar 07, 2023, 10:08 AM	http://kidsparadise.org/		ht	tps://app.recordedfuture.com/live/sc/notification/?ld=qR7g8n	Professional Services Development - Professional Services	ices Dev	elopme	nt
ar 07, 2023, 10:08 AM	http://appleorigin.com/		ht	tps://app.recordedfuture.com/live/sc/notification/?id=qR7g8n	Professional Services Development - Professional Services	ices Dev	elopme	nt
ar 07, 2023, 10:08 AM	http://ahfc.com.cn/		ht	tps://app.recordedfuture.com/live/sc/notification/?id=qR7g8n	Professional Services Development - Professional Services	ices Dev	elopme	nt
ar 07, 2023, 10:08 AM	http://saudiaramco.fr/		ht	tps://app.recordedfuture.com/live/sc/notification/?id=qR7g8n	Professional Services Development - Professional Services	ices Dev	elopme	nt
ar 07, 2023, 10:08 AM	http://vorweggeher.de/		ht	tps://app.recordedfuture.com/live/sc/notification/?id=qR7g8n	Professional Services Development - Professional Services	ices Dev	elopme	nt
ar 07, 2023, 10:08 AM	http://new.veranstaltungsundme	essebau.de/	ht	tps://app.recordedfuture.com/live/sc/notification/?id=qR7g8n	Professional Services Development - Professional Services	ices Dev	elopme	nt
ar 07, 2023, 10:08 AM	http://secure2help-paypal.com/		ht	tps://app.recordedfuture.com/live/sc/notification/?id=qR7g8n	Professional Services Development - Professional Services	ices Dev	elopme	nt

Recorded Future - Potential Logo Abuse Detection

Recorded Future - Vulnerability Risk, New Critical or Pre NVD Watch List Vulnerabilities

This single dashboard combines the Tech Stack - Vulnerability Risk, New Critical or Pre NVD Watch List Vulnerabilities and the Global - Vulnerability Risk, New Critical or Pre NVD Watch List Vulnerabilities alert rules, one for table. The alerts are sorted by Criticality Level and display the CVE that triggered the alert, the severity and a description. If the Description field is empty we have provided the nvd.com link.

Recorded	Future - Vulnerability	Risk, New Critica	al or Pre NVD Watch List Vulnerabilities 🎽	۲	RR :	t (3 :
100	D	ays					
Tech Stack - Vuln 1 minute ago	erability Risk, New C	ritical or Pre NVI	D Watch List Vulnerabilities				÷
Nov 09, 2022	CVE-2022-41128	- Very Critical	https://mwl.niet.aov/unilo/datai/JCVE.2022.41128				
Nov 09, 2022	CVE-2022-41125	Very Critical	mpp/meta/spar/sequences/s				
0+06 2022	CVE-2022-35014	Very Critical	nicpsymposianicgory publication on the text of the text stand module for CLD1 through 10.0.2 silour BUD code interties				
0++ 21 2022	CVE-2022-33714	Very Critical	prevision minimaredynamiared rescape in normaniared include to GLF1 model actives Fire Code injection.				
New 28, 2022	CVE-2022-3723	very critical	mups. Jimou most govy young de ange yee 2022 23 23 A subservision of and a finite state of the constant of the state and description of the state of the state state state state of the state of the state				
NOV 28, 2022	CVE-2022-4088	High	A vulnerability was found in ficksy stock management system and classified as critical. Anected by rins issue is some unknown functionality of the file (pages/processiogin.pnp). In en	aniputa	ition of t	ne arg	a
Nov 23, 2022	CVE-2022-4093	High	SQL injection attacks can result in unauthorized access to sensitive data, such as passwords, credit card details, or personal user information. Many high-profile data breaches in recer	t years	have be	en the	r
Nov 21, 2022	CVE-2022-4051	High	A vulnerability has been found in Hostel Searching Project and classified as critical. This vulnerability affects unknown code of the file view-property.php. The manipulation of the argu	ment p	operty_	id lead	s
Nov 21, 2022	CVE-2022-4070	High	Insufficient Session Expiration in GitHub repository librenms/librenms prior to 22.10.0.				
Nov 17, 2022	CVE-2022-40127	High	A vulnerability in Example Dags of Apache Airflow allows an attacker with UI access who can trigger DAGs, to execute arbitrary commands via manually provided run_id parameter. The	s issue	affects	Apach	e
Global - Vulneral	sility Risk, New Critica	al or Pre NVD Wa	ntch List Vulnerabilities				1
1 minute ago		Mala ana bilita					
Time	Vulnerability ID	Level	Vulnerability Description				
Nov 29, 2022	CVE-2022-4135	Very Critical	Heap buffer overflow in GPU in Google Chrome prior to 107.0.5304.121 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escap	ie via a	crafted	HTML	page
Oct 27, 2022	CVE-2022-42827		https://nvd.nist.gov/vuln/detail/CVE-2022-42827				
Nov 09, 2022	CVE-2022-41091	Very Critical	https://nvd.nist.gov/vuln/detail/CVE-2022-41091				
Nov 09, 2022	CVE-2022-41073		https://nvd.nist.gov/vuln/detail/CVE-2022-41073				
Nov 29, 2022	CVE-2022-0698	Very Critical	Microweber version 1.3.1 allows an unauthenticated user to perform an account takeover via an XSS on the 'select-file' parameter.				
Nov 09, 2022	CVE-2022-41128	Very Critical	https://nvd.nist.gov/vuln/detail/CVE-2022-41128				

Vulnerability Risk, New Critical and Pre NVD Watch List Vulnerabilities

Supported Alerts

Recorded Future Intelligence Goals Library Alerts are supported and DSM mapped by default. For a complete list of supported alerts please refer to the Appendix.

In order to parse custom alerts utilise the DSM Editor to map the custom alerts to a new QID. For more information please refer to Mapping custom alerts using the DSM Editor.

Mapping custom alerts using the DSM Editor

- 1. Click on the Log Activity tab
- 2. Select one or more events that are shown as Unknown
- 3. From the Actions list select DSM Editor.

Search V Quick Searches V	⁷ Add Filter 🛛 拱 Save Criteria	🗧 🕒 Save Results 🔗 Cancel 🦄	p False Positive Rules	 Acti 	ons 🔻		
				-	Show All		
Advanced Search •					Export to XML	►	
					Export to CSV		
				8	Delete		
				- <u> </u>	Notify		
				a	Print		
Original Filters:				0	Historical Correlation		
Log Source Type is Recorde	ed Future Alerts (Clea	r Filter)			DSM Editor		
Current Filters:					Edit payloads by	og so	urce type
Low Level Category is Unkn	own (Clear Filter)						
Current Statistics							
Total Results 115 (24 Data Files Searched Subsea	7.1KB Total) Ca arch (No Data Files) In	ompressed Data Files Searched dex File Count	Subsearch (No Cor Subsearch (No Inde	npresse x Files)	d Data Files) Duratio More D	n)etails	5ms
	Event Name	Log Source	Event Count		Time 🔻		Low Level Category
	Unknown	Recorded Future Alerts	1	21 Nov	2022, 06:59:15		Unknown
	Unknown	Recorded Future Alerts	1	21 Nov	2022, 06:59:15		Unknown

4. Click on the Settings icon (bottom right hand side) and select the following fields: Event Category, Event ID, Event Name, Low Level Category.

Soloot All		
Email in Code Repo (custom)		
Email Leaked (custom)		
Email Leaked - Email (custom)	0 0 0 0 0 0 0 0 0	
Event Category	0 0 0 0 0 0 0 0 0	
V Event ID	0 0 0 0 0 0 0 0 0	
Event Name*	0 0 0 0 0 0 0	
Fragment (custom)	0 0 0 0 0 0 0 0 0	
Global Vulnerability Criticality (c	ustom)	

5. Review the Log Activity (Preview) pane. The DSM will have Event Category and Event ID extracted and ready to go as shown below:

Log Activity Preview (Parsed but not Mapped:2/2)

A preview of the payloads in the Workspace as they would appear in the Log Activity viewer using the current configuration.

Event Category	Event ID	Event Name*
rf_alert	Custom rule - Brand Mentions	Unknown
rf_alert	Custom rule - Typosquatting	Unknown

6. Click on the Event Mappings tab

7. Click on the blue plus icon "+"

Properties	Event Mappings	Configuration	
Filter			+
		Advanced Filter	A

8. Select the corresponding Event Category and Event ID combination, for example:

Create a new Event Mapping

Enter an Event ID and Event Category combination to map to a QID record. A QID record allows a human-meaningful name and description to be associated with an event, as well as a Low Level Category and Severity value, which can in turn be used to trigger rules and building blocks.

This table lists the Event ID/Event parsed from events within the Wor corresponding Event Mapping. Thi that should be created for all even successfully. Click on a row in this Event Category values into the con	Category combination kspace that do not construct the space that do not construct the space of t	ons that are surrently have a Event Mappings ace to parse rent ID and ds below.
Event ID	Event Category	
Custom rule - Brand Mentions	rf_alert	
Custom rule - Typosquatting	rf_alert	
Event ID 1		
Event ID 1 Custom rule - Brand Mentions		
Event ID 1 Custom rule - Brand Mentions Event Category 1 rf_alert		
Event ID ① Custom rule - Brand Mentions Event Category ① rf_alert QID Record Choose QID		

9. Click Choose QID...

- 10. Click Create New QID Record
- 11. Provide the new QID record with the necessary information, such as name, description, high and low level categories, for example:

QID Records

Create New QID Record

Name	Log Source Type
Alert - Brand Mentions (custom)	Recorded Future Alerts -
Description	High Level Category
This is a custom alert to track brand mentions on the dark web.	Suspicious Activity -
	Low Level Category
	Suspicious Activity
	Severity 3 *
	Save 4 Go Back

- 12. Click Save
- 13. Select the newly created QID and click OK
- 14. Click Create
- 15. Click Save

讠 To find out more about the DSM Editor, please visit 🐵 DSM Editor overview

Logging & Troubleshooting

Please refer to the following URL for instructions on how to download QRadar Application logs. https://www.securitylearningacademy.com/course/view.php?id=4818

Additionally, application logs are available in the application configuration page.

Recorded Future Settings								
	Configuration retrieved successfully	Save						
Recorded Future API								
API Key								
Provide a Recorded Future API key to authenticate this application. Reach out to <u>Recorded Future Support</u> to retrieve your key. SSL Verification								

Syslog connection issues

Verify application container can reach the syslog destination via TCP 514.

- 1. Connect to the backend of QRadar console / App Node
- 2. Open a shell inside the application container

1 /opt/qradar/support/recon connect <app id>

3. Send a test syslog message

1 nc -w 0 <syslog destination ip> 514 <<< "Syslog-test-message"</pre>

4. On the QRadar Console run a payload search for Syslog-test-message and verify the test message is found.

5. If the the above steps fail, then verify network routing and firewall settings.

Logs indicate alerts were sent to QRadar, but search returns no alerts

After alert events have been sent to QRadar via Syslog the Event Pipeline in QRadar needs to process and store those events, this cane take several minutes. Meaning that a search might not find the events that have been ingested a minute ago. Wait for a few minutes and try again.

Truncation of events

Not all Recorded Future alerts are equal and some are rather large and might get truncated by the QRadar event pipeline. Try increasing the **Max TCP Syslog Payload Length** from 12K to a larger value, but please do so careful and involve IBM QRadar Support if needed as increasing the size can have a negative impact on the performance of QRadar.

To increase the Max TCP Syslog Payload Length, click here.

Reference: QRadar: TCP and UDP Syslog Maximum Payload Message Length for QRadar Appliances

Not fetching alerts

The integration only fetches alerts with a status of no-action or as shown in the portal New. Verify that the alerts you wish to fetch have this status set.

Appendix

Supported Alert Rules

- Analyst-On-Demand Report
- · Banking and Payments, Attackers in Banking & Payments Cyber Attacks
- · Banking and Payments, Malware Used in Banking & Payments Cyber Attacks
- · Banking and Payments, Banking Trojans, ATM Malware, Exploit Kits Malware
- Banking and Payments, Trending Targets in Banking & Payments
- · Banking and Payments, Vulnerabilities Recently Related to Banking & Payments
- · Brand name in suspicious websites content (OCR)
- Brand on Cyber-Focused Messaging Channels
- Brand Mentions with Cyber entities
- Company Email on Code Repository
- Credit Card Monitoring
- Cyber Espionage, RATs, Exploits, and Rootkits
- Cyber Espionage, Related Targets
- Cyber Espionage, Related Vulnerabilities
- Cyber Espionage, APT Threat Actors
- Cyber Events affecting my Brands
- Domains on Code Repositories
- Executive Impersonation on Social Media
- · Executive Impersonation on professional networking website
- Exploit Kit Modification
- Gift Card Monitoring
- Global Third-Party Risk, Risk
- Global Third-Party Risk, Trend
- Global Trends, Trending Attackers
- Global Trends, Trending Operations
- Global Trends, Trending Vulnerabilities
- Global Trends, Trending Methods
- Global Trends, Trending Targets
- · Global Vulnerability Risk, New Critical or Pre NVD Vulnerabilities
- · Global Vulnerability Risk, Vendors and Products Mentioned with Vulnerabilities
- · Global Vulnerability Risk, Vulnerabilities Recently Linked to Malware
- · Global Vulnerability Risk, Vulnerabilities Recently Linked to Pentest Tools
- · Global Vulnerability Risk, Vulnerabilities, New Exploit Chatter
- ICS/SCADA, ICS Malware, RATs
- ICS/SCADA, Trending Targets in ICS/SCADA
- ICS/SCADA, Vulnerabilities Related to ICS/SCADA Cyber Attacks
- ICS/SCADA, Attackers in ICS/SCADA Cyber Attacks

- · ICS/SCADA, Malware Used in ICS/SCADA Cyber Attacks
- IP Address Mentions
- Identify Similar Domains
- Increased Domain Risk Score
- Increased IP Address Risk Score
- Industry Risk, Trending Attackers in Industry
- Industry Risk, Trending Companies in Industry
- · Industry Risk, Trending Industry Peers in Watch List
- · Industry Risk, Trending Methods in Industry
- · Infrastructure and Brand Risk, Brand Names in Watch Lists
- Infrastructure and Brand Risk, Potential Typosquatting Watch List Domains
- Leaked Credential Monitoring
- Leaked Email Monitoring
- Mentions of Service Disruptions
- My brands on Dark Web and closed sources
- · My domains on Dark Web and closed sources
- Phishing or Spam Campaigns (Phishing Related to Operations)
- Possible Fake Apps Detection
- Potential Logo Abuse Detection
- · Ransomware, Software Recently Linked to Ransomware
- · Ransomware, Vulnerabilities Recently Linked to Ransomware
- Target Trends, Trending Attackers Linked to Targets
- Target Trends, Trending Methods Linked to Targets
- Target Trends, Trending Operations Linked to Targets
- Target Trends, Trending Related Attackers
- Target Trends, Trending Targets in Watch List
- Third-Party Risk, Risk
- Third-Party Risk, Trend
- · Trends, Trending Operations in Watch List
- Trends, Trending Watch List Attackers
- Trends, Trending Watch List Methods
- Trends, Trending Watch List Operations
- Trends, Trending Watch List Targets
- Trends, Trending Watch List Vulnerabilities
- Vulnerability Risk, Watch List Vendors & Products Mentioned with Vulnerabilities
- · Vulnerability Risk, New Critical or Pre NVD Watch List Vulnerabilities
- · Vulnerability Risk, Watch List Vulnerabilities Linked to Pentest Tools
- · Vulnerability Risk, Watch List Vulnerabilities New Exploit Chatter
- · Vulnerability Risk, Watch List Vulnerabilities Recently Linked to Malware
- Vulnerability Risk, Watch List Vulnerabilities with Proof of Concept code available

Out-of-the-box Custom Event Properties (CEP)

- Alert Category
- Alert ID

- Alert Priority
- Alert Rule Name
- Alert Seq
- Alert Seq Total
- Alert Source Name
- Alert Title
- Alert Triggered Time
- Alert URL
- Alert Updated Time
- DNS A Record IP
- DNS A Record IP Info
- DNS A Record IP Risk Score
- DNS NS
- Domain Abuse Context
- Domain Code Repo
- Email Leaked
- Email Leaked Email
- Email in Code Repo
- Entity Criticality
- Entity Subject
- Entity Risk Score
- Fragment
- Global Vulnerability Criticality
- Global Vulnerability Description
- Global Vulnerability ID
- Global Vulnerability Level
- Global Vulnerability Source URL
- Latest Screenshot
- Leaked Password
- Logo ID
- Logo URL
- MX Domain
- MX Domain Info
- MX Domain Risk Score
- Owner Name
- Repo Source Author
- Repo URL
- RF Organisation
- Similar Domain
- Status In Portal
- Targets List
- Whois City
- Whois Country
- Whois Name
- · Whois State